



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/562,775	04/10/2006	Dieter Jorgens	P05,0424	7977
26574	7590	06/15/2009		
SCHIEF HARDIN, LLP PATENT DEPARTMENT 6600 SEARS TOWER CHICAGO, IL 60606-6473			EXAMINER GERGISO, TECHANE	
			ART UNIT 2437	PAPER NUMBER
			MAIL DATE 06/15/2009	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

### Office Action Summary

**Application No.**

10/562,775

**Applicant(s)**

JORGENSEN ET AL.

**Examiner**

TECHANE J. GERGISO

**Art Unit**

2437

**Period for Reply** -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 06/02/2009.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 24-50 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 24-50 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SI/02)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### DETAILED ACTION

1. This is a Final Office Action in response to the applicant's communication filed on June 02, 2009.
2. Claims 24-50 have been examined and are pending.

### *Response to Arguments*

3. Applicant's arguments filed June 02, 2009 have been fully considered but they are not persuasive.

In response to the Office action correspondence the applicant argues that (remark: page 1):

*"First, claim 24 recites not storing that the encrypted sensitive data in a readable decrypted form but rather storing the encrypted sensitive data in a non-volatile memory such that the decrypted sensitive data are distributed in a plurality of memory segments with a non-volatile memory. By storing the decrypted sensitive data in a plurality of memory segments it is rendered not readable. Nowhere does Campagna or Wiley describe such a plurality of memory segments to make the data not readable. Wiley in Figure 3 merely shows encryption at 802, storage in a memory 803, and then the print mechanism 800. But there is no discussion anywhere of a distributed storage in a plurality of memory segments to make the decrypted sensitive data non-readable. Campagna only discusses the decrypted data controlling control signals for the printer. It is further noted the Examiner nowhere cites Applicants' claim language quoted above with an attribution of that claim language in either reference"*

The examiner disagrees with the applicant's argument and analysis for the following reasons: In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e.,

*not storing that the encrypted sensitive data in a readable decrypted form but rather storing the encrypted sensitive data in a non-volatile memory such that the decrypted sensitive data are distributed in a plurality of memory segments with a non-volatile memory*)

are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Claim 24 recited as follows is different from features upon which applicant relies on in the applicant's argument.

24. (new) A method for printing of sensitive data, comprising the steps of:

not storing the decrypted sensitive data in a readable decrypted form after the decrypting but before printing of the data, but rather storing the decrypted sensitive data in a non-volatile memory such that the decrypted sensitive data are distributed in a plurality of memory segments of the non- volatile memory where a relationship of the memory segments in the non-volatile memory is stored as relationship data independently of the stored decrypted sensitive data;

In addition the applicant argues (remark: page 2) that:

“Next claim 29 distinguishes by reciting that *a relationship of the memory segments in the non-volatile memory is stored as relationship data independently of the stored decrypted sensitive data*. This makes the decrypted sensitive data non- readable since without the relationship with the memory segments one could not read the memory segments in the proper sequence. Nowhere is this shown anywhere in Wiley or Campagna and the Examiner also does not provide any attribution in either reference for this claim language.”

Again the examiner disagrees with the applicant’s argument and analysis for the following reasons: In response to applicant’s argument that the references fail to show certain features of applicant’s invention, it is noted that the features upon which applicant relies (i.e.,

*a relationship of the memory segments in the non-volatile memory is stored as relationship data independently of the stored decrypted sensitive data*)

are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Claim 29 recited as follows is different from features upon which applicant relies on in the applicant’s argument.

29. (new) A method according to claim 24 wherein the decryption and the conversion into control signals are executed in immediate temporal succession.

Furthermore, the examiner would like to note that during examination the claims are given the broadest reasonable interpretation in light of the applicant's disclosure and the following claimed and argued features

*storing the decrypted sensitive data in a non-volatile memory such that the decrypted sensitive data are distributed in a plurality of memory segments of the non-volatile memory where a relationship of the memory segments in the non-volatile memory is stored as relationship data independently of the stored decrypted sensitive data*

are considered accordingly and can be interpreted to be performed by the workstation's Operating System Software, File System and Storage Controllers or Memory Access Modules that stores any data including *the decrypted sensitive data in a non-volatile memory such that the decrypted sensitive data are distributed in a plurality of memory segments of the non-volatile memory in a non-sequential or non-consecutive memory space* and therefore consecutive data (decrypted data, for that matter encrypted data also) are stored in a plurality of distributed non-volatile memory segments in a non-consecutive or non-sequential manner. Such technique of memory usage and memory addressing are a well known and established technique to one of ordinary skill in the art at the time of invention.

Non-volatile memory, or non-volatile storage, is computer memory that can retain the stored information even when not powered. Examples of non-volatile memory include read-only memory, flash memory, most types of magnetic computer storage devices (e.g. hard disks, floppy disks, and magnetic tape), optical discs.

In its broadest interpretation, the claimed features and alleged limitations are related to Memory management (the act of managing computer memory) for any type of data (including

decrypted sensitive data) using memory controllers and Operating systems. Therefore, for at least the above reasons, the applicant's arguments are not persuasive to overcome the prior arts in record and place the independent claims in condition for allowance including their corresponding dependent claims.

### ***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 24-29 and 41-50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiley et al. (hereinafter referred to as Wiley, US. Pub. No.: 2003/0154383) in view of Campagna et al (hereinafter referred to as Campagna, US Pub. No.: 2003/0081775)

As per claim 24:

Wiley discloses a method for printing of sensitive data, comprising the steps of:

at a workstation encrypting sensitive data to be printed (0129; encrypted file sent by sending computer entity);

transferring to a printing device having a printing unit the encrypted sensitive data to be printed (0129; encrypted file sent by sending computer entity; 0131);

decrypting the sensitive data to be printed to create decrypted sensitive data (0131; the printer decrypts the file);

storing the decrypted sensitive data in a non-volatile memory such that the decrypted sensitive data are distributed in a plurality of memory segments of the non-volatile memory where a relationship of the memory segments in the non-volatile memory is stored as relationship data independently of the stored decrypted sensitive data (0021; 0030; 0131; 0132; local memory for storing image data; 0140; raster pages for printing); and

printing the decrypted sensitive data with the printing unit on a recording medium (0140; printing page at a time).

Wiley does not explicitly disclose converting the decrypted sensitive data to be printed into control signals for activation of the printing unit; not storing the decrypted sensitive data in a readable decrypted form after the decrypting but before printing of the data. Campagna, in analogous art, however discloses converting the decrypted sensitive data to be printed into control signals for activation of the printing unit; not storing the decrypted sensitive data in a readable decrypted form after the decrypting but before printing of the data (0037; decrypt control signal). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Wiley to include converting the decrypted sensitive data to be printed into control signals for activation of the printing unit; not storing the decrypted sensitive data in a readable decrypted form after the decrypting but before printing of the data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a method



and system for securing the link between the accounting device and printer of a closed system meter that is cost efficient and easy to implement as suggested by Campagna in (0010).

As per claim 41:

Wiley discloses a system for printing sensitive data which have been encrypted, comprising:

a printing device having a printing unit connected to a controller (0129; encrypted file sent by sending computer entity);

said controller receiving said encrypted sensitive data; said controller comprising a decryption module, a non-volatile memory, a relationship data memory (0131; the printer decrypts the file), and

storing the decrypted sensitive data in said non-volatile memory such that the decrypted sensitive data are distributed in a plurality of memory segments of the non-volatile memory, and wherein a relationship of the memory segments in the non-volatile memory is stored as relationship data in said relationship data memory independently of the stored decrypted sensitive data (0021; 0030; 0131; 0132; local memory for storing image data; 0140; raster pages for printing).

Wiley does not explicitly disclose a converter which converts decrypted sensitive data from said decryption module into control signals for activation of said printing unit; and in said controller not storing the decrypted sensitive data in a readable decrypted form after the decrypting, but before printing of the data. Campagna, in analogous art, however discloses a

converter which converts decrypted sensitive data from said decryption module into control signals for activation of said printing unit; and in said controller not storing the decrypted sensitive data in a readable decrypted form after the decrypting, but before printing of the data (0037; decrypt control signal). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Wiley to include a converter which converts decrypted sensitive data from said decryption module into control signals for activation of said printing unit; and in said controller not storing the decrypted sensitive data in a readable decrypted form after the decrypting, but before printing of the data. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a method and system for securing the link between the accounting device and printer of a closed system meter that is cost efficient and easy to implement as suggested by Campagna in (0010).

As per claims 25 and 42:

Wiley discloses a method, wherein said decrypted sensitive data is stored in said non-volatile memory as said control signals representing said decrypted sensitive data (0138).

As per claims 26 and 43:

Wiley discloses a method, wherein the step of relating the memory segments using said relationship data and then printing the decrypted sensitive data (0132).

As per claims 27 and 44:

Wiley discloses a method, wherein the relationship data is stored in a volatile memory (Figure 8: 803 memory).

As per claim 45:

Wiley discloses a system, wherein the printing unit comprises a character generator (0136; raster image process; 0137; 0140).

As per claim 46:

Wiley discloses a system, wherein the controller comprises at least one raster module as said converter (0136; raster image process; 0137; 0140).

As per claim 47:

Wiley discloses a system, wherein the controller comprises a combined decryption/raster module (0136; raster image process; 0137; 0140).

As per claims 28 and 48:

Campagna discloses a method, wherein the control signals containing decrypted sensitive data are stored in a volatile memory (0037).

As per claim 29:

Campagna discloses a method, wherein the decryption and the conversion into control signals are executed in immediate temporal succession (0014-0016).

As per claim 30:

Campagna discloses a method, wherein the decryption and the conversion into control signals is executed in a controller for activation of a character generator (0014-0016).

As per claim 49:

Wiley discloses a system, wherein a sensor for detection of recording media with predetermined security features is arranged on a transport path for recording media in a region before the printing unit such that the printing of sensitive data can be stopped given detection of recording media without security features (0140-0106).

As per claim 50:

Wiley discloses a method for printing of sensitive data, comprising the steps of:  
transferring to a printing device having a printing unit encrypted sensitive data to be printed (0129; encrypted file sent by sending computer entity);

decrypting the sensitive data to be printed to create decrypted sensitive data (0131; the printer decrypts the file);

storing the decrypted sensitive data in a non-volatile memory such that the decrypted sensitive data are distributed in a plurality of memory segments of the non-volatile memory where a relationship of the memory segments in the non-volatile memory is stored as relationship data independently of the stored decrypted sensitive data; and printing the decrypted

sensitive data with the printing unit on a recording medium (0021; 0030; 0131; 0132; local memory for storing image data; 0140; raster pages for printing).

Wiley does not explicitly disclose converting the decrypted sensitive data to be printed into control signals for activation of the printing unit. Campagna, in analogous art, however discloses converting the decrypted sensitive data to be printed into control signals for activation of the printing unit (0037; decrypt control signal). Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to modify the system disclosed by Wiley to include converting the decrypted sensitive data to be printed into control signals for activation of the printing unit. This modification would have been obvious because a person having ordinary skill in the art would have been motivated to do so to provide a method and system for securing the link between the accounting device and printer of a closed system meter that is cost efficient and easy to implement as suggested by Campagna in (0010).

6. Claims 31-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wiley et al. (hereinafter referred to as Wiley, US. Pub. No.: 2003/0154383) in view of Campagna et al (hereinafter referred to as Campagna, US Pub. No.: 2003/0081775) and in further view of Snyders (US Pub. No.: 2004/0080772 A1).

As per claim 31:

Wiley and Campagna do not explicitly teach print data are provided comprising both said sensitive data and non-sensitive data. Snyders, in an analogous art, however print data are

provided comprising both said sensitive data and non-sensitive data (0083). Therefore, it would have been obvious to a person in the art at the time the invention was made to modify the system disclosed by Wiley and Campagna to include print data are provided comprising both said sensitive data and non-sensitive data. This modification would have been obvious because a person having ordinary skill in the art, at the time the invention was made, would have been motivated to do to provide a system and method for securing and tracking a document transmitted over an open network and a printing facility connected to the customer along a workflow path as suggested by Snyders (0008).

As per claim 32:

Snyders discloses a method, the print data to be printed are transferred to the printing device in the form of a print data stream, the print data stream being converted into an intermediate language in the printing device, and the print data being converted into control signals (0004; 0005; 0016).

As per claim 33:

Snyders discloses a method, wherein the sensitive data and the non-sensitive data are connected into one data unit before transfer to the printing device (0083).

As per claim 34:

Snyders discloses a method, wherein the sensitive data are identified in the data unit via markings (0083).

As per claim 35:

Snyders discloses a method, wherein a layout that comprises regions to receive sensitive data is generated using the non-sensitive data (0083).

As per claim 36:

Snyders discloses a method, wherein the sensitive data are already encrypted before combination with the non-sensitive data into said one data unit (0051; 0057; 0058).

As per claim 37:

Snyders discloses a method, wherein the sensitive data are encrypted after combination with the non-sensitive data into said one data unit (0051; 0057; 0058).

As per claim 38:

Snyders discloses a method, wherein only the sensitive data are encrypted (0051; 0057; 0058).

As per claim 39:

Snyders discloses a method, wherein both the sensitive data and the non-sensitive data are encrypted (0051; 0057; 0058).

As per claim 40:

Snyders discloses a method, wherein the conversion of the sensitive data to be printed into control signals for activation of the printing unit via rastering of the data to be printed into one or more raster images is executed, whereby the raster images represent the control signals (0051; 0057; 0058).

### **Conclusion**

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See the notice of reference cited in form PTO-892 for additional prior art.

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.



### **Contact Information**

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to TECHANE J. GERGISO whose telephone number is (571)272-3784 and fax number is ~~(571) 273-3784~~. The examiner can normally be reached on 9:00am - 6:00pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Techane J. Gergiso/

Examiner, Art Unit 2437

/Emmanuel L. Moise/

Supervisory Patent Examiner, Art Unit 2437